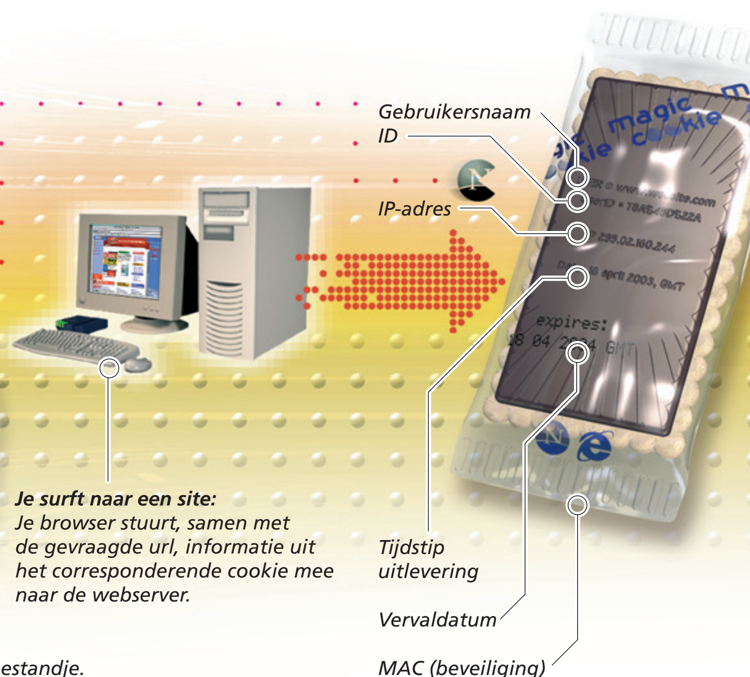
Alles over het hoe en waarom van cookies

De koekjestrommel

Ben je ooit op een website beland waar je begroet werd met je naam en voornaam? Wellicht heb je je afgevraagd hoe die site weet wie jij bent. Dat is het werk van cookies. Wat zo'n koekje doet en hoe het in elkaar zit, weet je na het verorberen van dit artikel.

Dankzij een cookie kan een website zien of jij die site al eens eerder bezocht hebt. Indien dat het geval is, kan het uitzicht van de site aangepast worden op basis van jouw eerder gemaakte voorkeuren. Zonder cookies zou elk bezoek dat jij aan een bepaalde website maakt, als het eerste bezoek gezien worden. Het gevolg daarvan is dat je elke keer opnieuw zou moeten ingeven dat je de Nederlandstalige versie van de site verkiest. Een cookie is niet meer dan een klein tekstbestandje op je harde schijf. In dat tekstbestandje worden enkele variabelen bewaard, die bij het aanroepen van een bepaalde pagina ingelezen worden. Met andere woorden: een cookie houdt je komen en gaan in het oog. Vermits een cookie niet meer dan een tekstbestandje is, is het ook niet gevaarlijk. Het is geen programma dat je harde schijf kan formatteren of allerlei ongure bewerkingen op je systeem kan loslaten. Het voordeel van een cookie ligt voor de hand. Aan de hand van cookies kan de webmaster zien hoe vaak jij naar die site terugkeert. Ook de lengte van je bezoek kan bewaard worden. Ofwel: wanneer elke bezoeker het na een halve minuut voor bekeken houdt, kan het bedrijf zich vragen beginnen stellen over het nut van haar website. Cookies worden ook gebruikt om reclame doeltreffender te maken. Een website kan de reclameboodschappen die het op jouw scherm tovert, aanpassen aan de gegevens die het uit de cookies haalt. Alle websites waar je iets kan kopen, maken gebruik van cookies. Je wordt begroet met je eigen naam, de website doet je aanbevelingen op basis van vorige aankopen die je verricht hebt. E-commercesites maken gebruik van zogenaamde 'winkelkarretjes'. Elk item dat jij koopt wordt aan het winkelkarretje toegevoegd. Tegelijk wordt het voorwerp samen met jouw ID in de database van de server opgeslagen. Aan de hand van dat ID kan de website jou identificeren. Het cookie bevat jouw ID en kan in de database van de server zien welke voorwerpen je allemaal wil kopen. Heb je een Delhaizekaart? Dat is precies hetzelfde principe. Al je aankopen worden nauwkeurig opgeslagen en op basis daarvan word je bestookt met reclame die aangepast is aan jouw voorkeuren. Iemand die reeds jaren Whiskas koopt, zal geen boodschap hebben aan reclame voor lekkere hondenbrokken. Kan je na het verwijderen van je cookies plots niet meer inloggen op je favoriete website? Dat komt omdat de website niet meer weet wie jij bent.





Je surft naar een site:
Je browser stuurt, samen met de gevraagde url, informatie uit het corresponderende cookie mee naar de webserver.

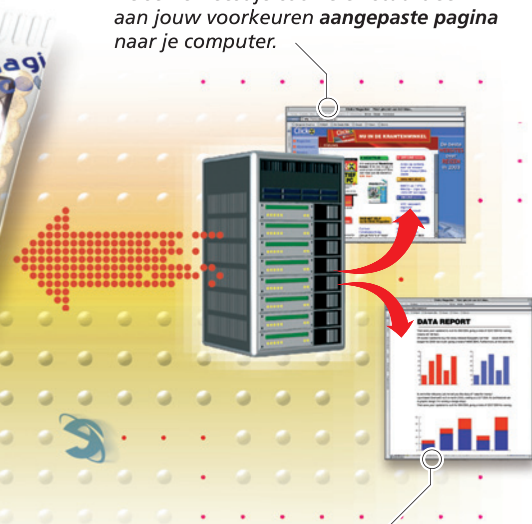
Een cookie is een ongevaarlijk tekstbestandje.

INFOGRAPHIC VEGAS ©

De server raadpleegt daarvoor immers het cookie dat je zopas gewist hebt. Ga dus naar de login-pagina van de desbetreffende website en geef opnieuw je identificatiegegevens in.

Magische koekjes

De naam cookie heeft helemaal niks te maken met het koekjesmonster uit Sesamstraat, maar verwijst naar de term magic cookie uit de Unix-wereld. Een magic cookie is een stukje code dat bij een programma hoort. De code is dynamisch van aard, wat wil zeggen dat die kan veranderen, afhankelijk van de acties die ondernomen worden. Dat geldt ook voor een internetcookie, vandaar dus de benaming. Wat gebeurt er nu concreet met zo'n cookie? Als je een website bezoekt, zijn er een aantal stappen die uitgevoerd worden. Eerst en vooral neemt jouw webbrowser contact op met de server van de webpagina die je wil openen. Tegelijkertijd zoekt je browser op je harde schijf naar een cookie van die website. Als je browser een cookie van die site terugvindt, worden de gegevens uit dat cookie naar de server verzonden, samen met de url van de pagina die jij wil bekijken. Wordt er geen cookie teruggevonden, dan verstuurt je browser enkel de url. De server ontvangt de url die jij opvraagt én de gegevens uit een (indien aanwezig) cookie. Als de webserver een cookie ontvangt, gebruikt het dat om je bijvoorbeeld een gepersonaliseerde pagina voor te schotelen. Is het je eerste bezoek, dan maakt de server een nieuw cookie aan, dat het vervolgens samen met de webpagina naar jouw computer verstuurt. Cookies hebben trouwens een eigenaardig neveneffect. Stel dat je een bepaalde website bezoekt en weigert om cookies van die pagina te accepteren. De server weet weliswaar dat je voor dit bezoek geen cookies wilt, maar omdat hij geen bestandje mag bewaren kan hij niet onthouden dat hij geen cookies mag bewaren. Gevolg hiervan is dat je bij het volgende bezoek dezelfde vraag voorgeschoteld krijgt.



*De server leest je cookie en stuurt een aan jouw voorkeuren **aangepaste pagina** naar je computer.*

*Je **surfgedrag** op deze site kan nauwkeurig geregistreerd worden.*

De binnenkant

Een cookie bevat doorgaans vijf variabelen. Ten eerste is er een ID, dat nodig is om jou te kunnen identificeren. Ook het tijdstip waarop het cookie uitgeleverd werd en de vervaldatum worden opgeslagen. Je *IP-adres* wordt eveneens bewaard. Tenslotte wordt ook een MAC (Message Authenticity Check)-code naar je cookie geschreven. Dat is een beveiliging die erop toeziet dat niet met de andere velden geknoeid is. Voor die code wordt gebruik gemaakt van een hash-algoritme. Meer uitleg over encryptie vind je op pagina 66 en in Clickx 34. Die beveiliging is nodig omdat cookies soms vertrouwelijke informatie bevatten. Dikwijls moet je een login en wachtwoord opgeven vooraleer je toegang krijgt tot een bepaalde site. Om de site gebruiksvriendelijker te maken, wordt een cookie naar je browser gestuurd. In dat koekje staat dat jij de rechtmatige gebruiker bent. Dat vermijdt dat je bij surfen binnenin de site telkens opnieuw je login en paswoord moet ingeven. Je cookie fungeert dus als toegangsticket tot de site. Iemand die dat cookie onderschept, heeft toegang tot jouw beveiligde zone. Dat is ook de reden waarom cookies een vervaldatum hebben. Indien een hacker je cookie onderschept, kan die dus slechts gedurende een bepaalde periode gebruik maken van het cookie. Bij een goed beveiligde verbinding zal het cookie samen met de overige data gecrypteerd worden. Een voorbeeld hiervan is SSL [www.ssl.com].

Een cookie van eigen deeg

Werk je met Internet Explorer, dan komen je cookies in txt-bestandjes terecht in de map Cookies, een submap van Windows of van \Documents and Settings\gebruikersnaam. Je zal zien dat jouw gebruikersnaam voor elk koekje staat. Voor gebruiker Filip krijgt een cookie van [www.amazon.com] dus de naam Filip@amazon.txt. Elke keer dat jij je browser opent, worden de cookies in het geheugen gelezen. Sluit je de browser, dan worden de cookies terug naar je harde schijf geschreven. Cookies waarvan de tijdspanne verloopt, worden van de harde schijf verwijderd. De reden voor die gebruikersnaam is om een onderscheid te kunnen maken tussen de verschillende gebruikers. Stel dat drie verschillende personen gebruik maken van één computer, alledrie loggen ze in op [www.amazon.com] en alledrie kiezen ze voor een andere voorkeurtaal, dan moet de computer weten welk koekje bij welke gebruiker hoort. Dat wordt verwezenlijkt door je gebruikersnaam als prefix te gebruiken. De gebruikersnaam wordt overigens niet naar de server verzonden. Enkel de gegevens in het tekstbestandje worden doorgestuurd. Op een cookie gelden ook bepaalde beperkingen. Zo mag een website enkel de cookies lezen die hij zelf geschreven heeft. Met 'zelf' bedoelen we alle cookies die aangemaakt zijn op hetzelfde domein.Dat betekent dat een cookie gemaakt door [www.amazon.com] niet gelezen kan worden door de server van pakweg [www.yahoo.com]. Omgekeerd geldt net hetzelfde, wat wil zeggen dat [www.yahoo.com] onmogelijk een

VAKTAAL

IP-adres: Afkorting van Internet Protocol-adres. Een IP-adres is een uniek adres dat wordt voorgesteld door vier getallen die door punten van elkaar worden gescheiden. Bijvoorbeeld: 188.165.237.32. Op die manier wordt iedere computer die op het internet is aangesloten, geïdentificeerd en kunnen deze pc's met elkaar informatie uitwisselen.

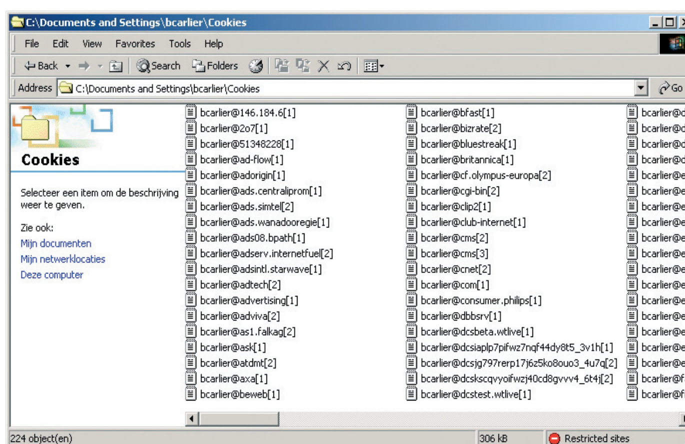
cookie kan maken voor het domein [www.amazon.com]. Nogal logisch, anders ligt de baan wijdopen voor allerlei oneerlijke praktijken. Een voorbeeld van meer controversiële praktijken is DoubleClick [www.doubleclick.com].

Dubieuze dubbelklik

DoubleClick bouwt een database op met profielen van gebruikers. Vervolgens krijgen de gebruikers reclameboodschappen gebaseerd op hun surfgedrag voorgeschoteld. Daarvoor heeft DoubleClick overeenkomsten met enkele duizenden websites gesloten. Dat zijn meestal websites op zoek naar een mogelijkheid om hun diensten of producten te promoten. Wanneer een website 'lid' wordt van DoubleClick, wordt hij een gastheer voor reclameboodschappen van alle leden van het DoubleClick-netwerk. Concreet wil dat zeggen dat op de website een link naar DoubleClick geplaatst wordt. Stel dat jij de startpagina [www.lycos.com] oproept. Daar staat een afbeelding die gelinkt is aan DoubleClick. Wanneer je browser [www.lycos.com] inlaadt, zal de afbeelding geladen worden vanop de server van DoubleClick. De afbeelding wordt willekeurig gekozen uit de database met partners. Dat wil zeggen dat de afbeelding (of advertentie) bij elke keer dat je de pagina opnieuw inlaadt (druk op F5) anders is. Wat is daar nu speciaal aan? Wel, de allereerste keer dat je een website bezoekt die geassocieerd is met DoubleClick, ontvangt jouw browser een cookie van de DoubleClick-server. Dat is een cookie met een uniek ID. Vanaf dan wordt elk bezoek van jou aan eender welke DoubleClick-website gelogd. DoubleClick herkent jouw ID en voegt het adres van de site toe in haar database. Na verloop van tijd heeft DoubleClick een mooie lijst van je surfgedrag opgebouwd.



Cookies: hebben ze iets te maken met het koekjesmonster?



Onze map met cookies.

Op basis daarvan kan het de advertenties die het op je scherm plaatst aanpassen. Eén van de websites die een overeenkomst heeft met DoubleClick is Lycos. Op de website [http://info.lycos.com/privacy/doubleclick. asp] kan je lezen dat onder meer je IP-adres en de trefwoorden die je gebruikt bij zoekacties bewaard worden om advertenties gerichter te maken. Wie zei daar iets over paranoïa? Begin 2002 zou het bedrijf het bewaren van de surfgeschiedenis van de gebruikers opgegeven hebben. De kosten voor het verkrijgen en verwerken van de data zouden te zwaar opwegen tegen de voordelen ervan. Hoe het vandaag precies zit, is niet helemaal duidelijk, maar op [www.doubleclick. com/privacy_policy/privacy.htm] kan je alvast alle DoubleClick-cookies uitschakelen. Klik op de afbeelding getiteld Ad cookie opt-out. Wij konden alvast een DoubleClick-cookie in onze map met Cookies terugvinden.

Cookies blokkeren

Werk je met Internet Explorer, dan komen je cookies in txt-bestandjes terecht in de map Cookies, een submap van Windows of van \Documents and Settings\gebruikersnaam. Je kan die bestanden zelf wissen, maar je kan dat ook overlaten aan de opdracht Cookies verwijderen. Die vind je in Internet Explorer, menu Extra, Internet-opties, tabblad Algemeen. Open meteen ook even het tabblad Privacy. Afhankelijk van waar je de schuifknop positioneert, kan je cookies blokkeren of toelaten. In de hoogste stand kan je zelfs álle cookies blokkeren, maar dan beperk je wel de functionaliteit van heel wat sites. Via de knop Bewerken kan je verder instellen welke cookies je per site wil blokkeren of toestaan. Tik het adres van een website in en kies dan voor Blokkeren of Toestaan. Deze optie is niet beschikbaar indien je alle cookies toelaat of allemaal blokkeert. Het is met andere woorden niet mogelijk een uitzondering op de regel in te stellen. We maken ook een onderscheid tussen directe en indirecte cookies. Directe cookies zijn afkomstig van een website die je ook daadwerkelijk hebt bezocht. Indirecte cookies worden op je schijf achtergelaten door bijvoorbeeld een reclamebanner die van een andere webserver afkomstig is dan degene die je bezoekt. Indirecte cookies kunnen dus ook komen van een website die jij nog nooit hebt bezocht. Afhankelijk van de instelling van de schuifbalk worden indirecte cookies geblokkeerd of doorgelaten. Ook via de knop Geavanceerd kan je indirecte cookies blokkeren. Klik op Automatische cookie-verwerking opheffen en selecteer het vinkje Blokkeren onder Indirecte cookies. Selecteer je Cookies per sessie altijd toestaan, dan laat je alle cookies toe waarvan de levensduur niet langer is dan je bezoek aan die website.

Roep hulp in

Er bestaan ook allerlei hulpprogramma's die cookies de toegang tot je computer kunnen ontzeggen. Op [www.thelimitsoft.com/cookie] kan je de 'Cookie Crusher' downloaden. Besef wel dat als je cookies uitschakelt, je heel wat websites niet zal kunnen bezoeken en/of af te rekenen krijgt met foutmeldingen. Een cookie kan immers enkel informatie verkrijgen die jij ergens ingetikt hebt. Niet alle cookies zijn per definitie slecht. Heel wat cookies zorgen gewoon voor een betere surfervaring. Nog meer info over cookies kan je vinden op [www.cookiecentral.com] of onder de Security-rubriek van het W3C [www.w3c.org]. Op de site van het W3C kan je het Platform for Privacy Preferences of P3P [www.w3.org/P3P/] erop nalezen. Dit is een standaard die het W3C aanbeveelt aan webontwikkelaars. Het doel van P3P is tweeledig. Ten eerste zorgt het ervoor dat websites het opvragen van gegevens op een duidelijke en ondubbelzinnige manier moeten doen. Ten tweede moet de gebruiker weten welke gegevens door de server opgevraagd worden, wat ermee gedaan wordt én welke gegevensopvragingen je kan weigeren en/of toelaten. Heel handig bij cookies... In de praktijk betekent dat dus dat op elke site wel vermeld staat wat er gebeurt, maar je zal er wel goed naar moeten zoeken... Om te besluiten: let op welke informatie je prijsgeeft en wis van tijd tot tijd je Cookies-map. Je weet maar nooit wie er meekijkt.

— Benjamin Carlier —